Review and Findings of Submitted Proposals

Issued by the Digital Transmission Discussion Group
Copy Protection Technical Working Group
Version 1.0
November 11, 1997

Scott Smyers
Sony US Research Laboratories

Brendan Traw
Platform Architecture Laboratory, Intel Corporation

"OUTSIDE COUNSEL'S EYES ONLY"

S 00023

This page is intentionally left blank.

Table of Contents

"OUTSIDE COUNSEL'S EYES ONLY"

S 00027

1. Introduction and overview

1.1 Scope and Goals of this recommendation

This recommendation was prepared by the Digital Transmission Discussion Group (DTDG) for submission to its parent organization known as the Copy Protection Technical Working Group (CPTWG).

The CPTWG, and it's subgroups of which the DTDG is one, is an ad hoc group made up of industry and company representatives interested in the issue of protecting the rights of copyright holders when their data is distributed to consumers in digital form. The DTDG was authorized by the CPTWG at the end of 1996 with the expressed purpose of defining a Data Protection System (DPS) capable of preventing the unauthorized use of copyrighted material by ordinary consumers in ways which involve the transmission of that material in digital form over interfaces compliant with the IEEE 1394-1995 High Performance Serial Bus standard, commercially available derivatives of that interface standard and commercially viable applications utilizing that interface standard.

In simpler terms, the DTDG was created to define a means of "keeping honest people honest" when such people operate consumer electronics devices, including personal computers, which transfer copyrighted material over the IEEE 1394 interface using an isochronous channel. Devices compliant with the DPS, at such times as they transmit data or receive data using the DPS via an isochronous channel on the IEEE 1394 interface, shall behave in a manner which prevents the unauthorized copying or other unauthorized use of the copyrighted material by the average consumer.

1.2 Overview of process

The CPTWG authorized the creation of the DTDG and assigned a chairman at the normal CPTWG meeting which was held on October 3, 1996. Thereafter, the timeline of DTDG activity proceeded approximately as outlined below. Please note that this chronology of events was recreated after the fact and may not therefore be complete or accurate.

October 3, 1996	CPTWG authorized the creation of the DTDG and assigned a chairman
October 25, 1996	First meeting of the DTDG
December 17, 1997	Second meeting of the DTDG
January 31, 1997	Third meeting of the DTDG - began drafting offical Call For Proposals; CFP discussions continue over email in the subsequent weeks
March 4, 1997	Fourth meeting of the DTDG - detailed review of draft CFP
March 11, 1996	CFP officially released from the DTDG
April 25, 1997	Deadline of CFP - received 11 proposals; proposals were distributed to interested parties during the subsequent weeks
June 3, 4, 5, 1997	Fifth meeting of DTDG to discuss proposals; 2 proposals officially turned over to the Data Hiding Sub Group (DHSG) of the CPTWG; Detailed presentations of remaining proposals by their proposers
July 9, 10, 1997	Sixth meeting of DTDG; Further discussion of proposals; Began developing a formal request for supplemental evaluation data to be distributed to remaining proposers
July 24, 1997	Official release of Request for Supplemental Evaluation Data, issued by the DTDG and addressed to the remaining proposers
August 19, 20, 1997	Seventh meeting of DTDG to review supplemental information from proposer; TI officially withdraws their proposal
September 18, 19, 1997	Eighth meeting of DTDG; Further review of supplemental information and detailed review of tabular representation of this information; Toshiba and Intel officially combine their proposals into a single proposal
October 30, 1997	Ninth meeting of DTDG; Review draft of recommendation

The Call For Proposals (CFP) which was developed by the DTDG and formally issued on March 11, 1997 is contained in Appendix B of this document. The CFP requests proposals for a DPS having the following 3 layers:

1) Copy Control Information (CCI) Layer - a means of carrying information along with the copyrighted content that expresses the intentions of the copyright holder with regard to the conditions under which an end consumer is authorized to make a copy

2) Authentication Layer - a means for compliant devices to establish the authenticity of another device prior to exchanging copyrighted data

3) Encryption Layer - a means of encrypting or scrambling the copyrighted information when it is transmitted between devices in digital form

The DTDG received 11 proposals to the CFP from the following organizations (in alphabetical order):

1) Hitachi
2) IBM

3) Intel

4) Matsushita

5) NEC

6) NDS

7) Philips

8) PictureTel

9) Sony

10) Texas Instruments

11) Toshiba

Since the time that the DTDG received proposals from these companies on April 25, 1997, some proposers have withdrawn their proposal while others have combined their proposal with those of other proposers. The table below lists the proposals which were active at the time that this recommendation was being prepared (in alphabetical order by company):

Hitachi/ Matsushita/ Sony	CCI layer: Combination of Sony and Matsushita CCI proposals Authentication layer: Sony key management and authentication method with addition of challenge/response and MEI elliptic curve public key for authentication within a PC and in other defined areas Encryption layer: Hitachi M6 plus Matsushita CCBC
Intel/ Toshiba	CCI layer: Unchanged from original Intel proposal Authentication layer: Intel proposal with Toshiba elliptic curve technology Encryption: Unchanged from original Intel proposal
NDS	Uncharged from original proposal
PictureTel	As originally proposed with incremental changes

1.3 Relationship to Other Standards Activities

The DTDG CFP requires that the DPS protect data when it is transmitted via an isochronous channel on an IEEE 1394 serial bus interface. This is a minimum requirement of the DTDG DPS, however, it is also acceptable if the DPS can protect data when it is transmitted in digital form over other media.

Given this minimum requirement, the work of the DTDG has been of some interest to various standards groups working in related areas. In some cases, other standards setting bodies have referenced the DTDG activity, or have implemented changes which anticipate the ultimate resolution of the copy protection issue and the establishment of a DPS in the CE and PC industries.

The following sections describe related industry standards and other activities which recognize the work of the DTDG and which may be affected by the establishment of an industry wide DPS.

1.3.1 IEEE P1394a

The IEEE P1394a committee is engaged in an officially sanctioned IEEE standards activity. The scope of the IEEE P1394a activity includes technical development of compatible extensions and/or clarifications and interpretations of the existing IEEE 1394-1995 standard.

During the course of the DTDG activity, the IEEE P1394a committee has been periodically briefed on the progress of the DTDG. The IEEE P1394a committee has considered additions to their subject standard to accommodate agreements reached in the DTDG on the CCI layer, but finally decided not to make any changes.

1.3.2 Open Host Controller Interface (OHCI)

The OHCI group is an ad hoc working group which is working to define an industry standard register level interface for interfaces between PCs and 1394.

Some members of the OHCI group have participated in discussions at the normal DTDG meetings. At this time, the OHCI group has decided to include in their specification a mechanism by which an OHCI compliant interface controller will recognize the exposed CCI bits and take appropriate action based on the setting of these bits.

1.3.3 IEC 61883-FDIS

This draft international standard defines a means of controlling consumer devices using IEEE1394 defined asynchronous transactions, and it defines a variety of digital data formats for use in transmitting digital audio and digital video data over an isochronous channel on the 1394 interface.

Some of the DTDG proposals for the encryption layer specify how the proposed encryption method interacts with the IEC61883 defined digital data formats. Due to the widespread market acceptance of the IEC61883 standard, it is likely that any DPS which operates on 1394 will have to explicitly accommodate the mechanisms defined in that standard.

1.4 Legal disclaimer

The purpose of this report is to provide a neutral technical input regarding to DPS to the Copy Protection Technical Working Group (CPTWG), and thereafter to the plenary group consisting of the member companies of the MPAA, CEMA, ITI and BSA which considers possible legislative recommendation to the Congress in relation with technological measures that restrict unauthorized acts in respect of copyright works. This report is provided without prejudice to the outcome of further discussions regarding associated non-technical considerations. This report does not constitute any warranty whatsoever, an offer of license to any proprietary rights or a commitment to implementation by the DTDG or any individual or company participating the DTDG as to any of the submitted proposals. The DTDG or any individual or company participating the DTDG shall, in no circumstance, have any obligation based on this report, or on any proposal attached hereto.

Developers are warned that no final decision has been made with regard to a DPS, and that any product implementation based on this recommendation or the accompanying proposals is purely speculative.

Readers are advised that the editors of this document are employed by Intel and Sony, who are also preparing submissions described herein.

1.5 Outline of Report

Section one of this report describes the scope of the DTDG discussions, the process which the DTDG has followed to date, the relationship between the work of the DTDG and other standards activities and the legal disclaimer.

Section two of this report gives an overview of cryptographic issues related to the DTDG work. This section is intended as a tutorial for readers not familiar with these concepts.

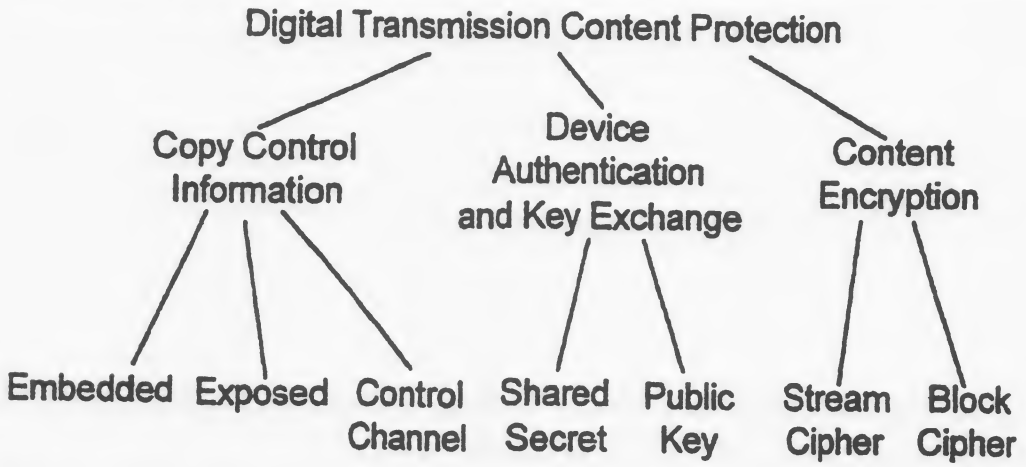
Section three provides an overview of the standing proposals. These overviews are limited to 200 words or less and were reviewed by the proposers.

Section four contains a set of tables which contain quantitative and other information about each of the standing proposals. This information was provided by each proposer in response to the request for supplemental evaluation data issued by the DTDG on July 24, 1997.

Section five documents the findings of the DTDG to date.

2. Technical Tutorial on Digital Transmission Content Protection

The DTDG Call for Proposals defined three layers which were intended to be used separately or in combination to protect the exchange of content across digital transmission mechanisms such as the IEEE 1394 serial bus. These layers are: Copy Control Information, Content Encryption, and Device Authentication and Key Exchange[1]. The following classification model has been developed to organize and describe the proposed solutions.



2.1 Copy Control Information (CCI)

The CCI layer provides a mechanism for exchanging the protection status of content being handled between devices. For example, video content may require the exchange of the CGMS, APS, and digital source bits[2]. The CCI must be exchanged in a robust manner to prevent its alteration. Should the CCI be alterable, a circumvention device could mislead a compliant device into believe that content originally marked "no copy" can be "copied once." Three different methods for exchanging CCI have been identified by the proposals submitted.

2.1.1 Embedded CCI

A range of techniques have been identified for exchanging CCI in a manner which is tightly coupled with the content. For instance, CCI is embedded in the transport mechanism for a particular content format, e.g. the MPEG transport stream. Additionally, techniques such as watermarking can be used to

[1] Originally, the CFP identified this layer as just Device Authentication leaving Key Exchange as a function not specifically associated with any particular layer. Since all proposals have chosen to address key exchange as part of the Device Authentication protocol, the definition of this layer will be expanded to include Key Exchange.

[2] For further information on the definition and function of these bits see Appendix A of the CFP.

embed the CCI directly into the content itself[3]. In both of these cases, the integrity of the Embedded CCI is ensured by the same method used to prevent the copying of the content itself (See Section 2.2).

2.1.2 Exposed CCI

CCI in Header.

The exposed CCI mechanism transports the CCI in manner such that it is available ("exposed") to devices which are not cognizant of any specific content formats. Although the CCI is expose for easy access, techniques are available to ensure that its integrity is maintained. A non format cognizant bit-stream recorder is an example of such a device. Content format independence is accomplished by putting the CCI in an exposed location such as in the 1394 packet header. When bits within the header of a particular digital transmission system are used to carry CCI, typically only a subset of the full CCI may be carried as there are only a small number of bits which can be assigned to this purpose.

Exposed CCI has been proposed as a means to ensure that format-cognizant devices do not make unauthorized copies of copy protected data. By comparing the information in the exposed CCI with the information in the embedded CCI, a format cognizant device can differentiate between an authorized use of a bit stream and an unauthorized copy of a bit stream.

2.1.3 Control Channel

OUT OF BAND. exchanged independently of the content.

The final method for exchanging CCI that has been identified by the proposals is via a control channel. This channel must be protected from tampering to ensure the integrity of the CCI by hashing, encryption, or other means. Control channels are capable exchanging large amounts of CCI, however, since the content and CCI are not sent over the same channel, synchronization must be provided between the CCI and the content itself.

2.2 Device Authentication and Key Exchange (AKE)

Process or means for a compliant Device to establish the authenticity of another device prior to exchanging copyrighted content or any encryption keys.

The AKE layer defines cryptographic protocols which are used by devices to determine the authenticity and compliance status of other devices with which content will be exchange. It is critical for a source device to verify the identity of destination devices to prevent the content from being sent to a circumvention device. In addition, the key exchange portion of the protocol provides a way to generate a shared key between two devices which can be use used to exchange content session keys.

The AKE process is based on a device's knowledge of a secret or secrets provided by a license authority and its ability to prove that it knows the secret without revealing it. A standard approach to proving knowledge of a secret is for the device initiating the authentication to send a random number to the device being authenticated. This random number is typically referred to as a random challenge. The device being authenticated modifies the random challenge in a manner determined by the device's secret and returns the modified value to the originator of the challenge. The originator can check the returned value to verify that the device being authenticated has access to the secret. If the value is correct, then the authentication has been successfully completed. The confidential exchange of cryptographic key can also be added to this basic challenge response protocol. Many variation on this basic protocol have been proposed. These variations are based on one of two fundamentally different cryptographic approaches which will be described in the following sections.

2.2.1 Shared Secret

Based on common set of secrets provided by a license authority and Symmetric Key Cryptographic Technology

The shared secret approach relies on a common set of secrets and symmetric key cryptographic technology. The secrets may be values or cryptographic functions which are generated and distributed by the license authority to device manufactures. When the secret is a value, it is used with a symmetric cipher to modify the random challenge issued during authentication. Secret functions are typically

---

[3] The applicability of watermarking and other related techniques to content protection are being evaluated by the CPTWG's Data Hiding Sub Group. Contact the tri-chairs of this sub group for additional information.

directly applied to the random challenge. When all compliant devices must contain the common secret to inter operate, it is considered a global shared secret.

2.2.2 Public Key

unique secret per device allocated by license authority.

A second approach is to base the AKE protocol on public key cryptographic techniques. Public key cryptography differs from symmetric key cryptography for AKE in that each device can have an unique secret (the device's private key) provided by the license authority yet still inter operate with other devices. The private key and a digital certificate signed by the license authority are used during the authentication process to prove the authenticity of the device. In addition, public key cryptography provides mechanisms for the exchange of keys as well as the capability to revoke the participation of compromised or rogue devices in the content protection system.

2.3 Content Encryption

Renders CONTENT a unusable prior to transmission

if copy is made copy is unusable.

To prevent the generation of usable copies of protected content, the content can be encrypted and decrypted at the end points of the digital transmission system. Content which is encrypted should be unusable by device which do not have the necessary keys to decrypt the content. In many digital transmission systems, such as the IEEE 1394 serial bus, all interconnected devices can receive any content being transferred. Unless the content is encrypted, non-compliant devices could make a copy. While public key cryptography could be used to protect the content, for performance reasons, all proposals have chosen to use symmetric key ciphers. These symmetric key ciphers can be divided into two classes: Stream and Block.

2.3.1 Stream Cipher

Same key used to encrypt and decrypt.

Stream ciphers apply a sequence of keys to transform individual data characters (e.g. typically bits or bytes).

2.3.2 Block Cipher

Block ciphers apply a fixed (key dependent) transformation to blocks of data.

3. Overview of Proposals

Each of the proposals submitted to the DTDG addresses all three of the layers described in the CFP. Within each layer, however, a range of solutions have been proposed. The proposal proponents agreed at the June 5th DTDG meeting that each of the three layers in their respective solution can be logically de-coupled from each other.

3.1 Hitachi/Matsushita/Sony

The Hitachi/MEI/Sony proposal covers all three layers of the DPS requested by the DTDG CFP.

3.1.1 CCI

Embedded CCI is mapped into an Encryption Mode Indicator (EMI) which indicates the encryption modes applied to the contents. EMI allows easy access to the CCI for all compliant devices and restricts their behavior for copy protected contents. Circumvention by changing the EMI bits will cause the decryption to fail, thus ensuring the integrity of the EMI.

3.1.2 Authentication

The combination of the Asymmetric and Public Key AKE and the Authentication Manager addresses the differences in PC and CE environments.

The asymmetric key AKE, which is mandatory between CE devices, utilizes the M6 block cipher and the asymmetric key distribution based on a pair of Service and License Key for each service the device supports. In this proposal, each sink device has a unique License Key, generated using the device's worldwide-unique Node_Unique_ID, defined in the IEEE1394-1995. Source devices hold the shared service keys for each service which the device supports.

The Public Key AKE is based on elliptic curve cryptographic technique which is mandatory between PC applications, while optional for use between 1394 devices.

3.1.3 Content Encryption

The M6 block cipher combined with MEI's converted-CBC is used.

3.2 Intel/Toshiba

The Intel/Toshiba proposal covers all three layers of the DPS requested by the DTDG CFP.

3.2.1 CCI

CCI is exchanged between devices via both embedded and control channel mechanisms. To ensure the integrity of CCI traversing the control channel, encryption, hashing, and sequence numbering techniques are used. This proposal is compatible with exposed CCI techniques which can ensure integrity, although no specific solution is specified.

3.2.2 Authentication and Key Exchange

A two phase mutual AKE process is proposed. The first phase of AKE (Preliminary Authentication) uses a shared secret technique based on the modified Blowfish cipher and the SHA-1 hash function. Following the successful completion of the first phase, content exchange is enabled and the second phase (Full Authentication) of the AKE process is initiated. The second phase uses established Public Key cryptographic techniques including the Digital Signature Standard and Diffie-Hellman Key Exchange based on an Elliptic Curve Cryptosystem. Certificate revocation is provided as an optional capability.

3.2.3 Content Encryption

This proposal can support multiple content ciphers. The specific cipher to be used for a given exchange of content is selected during AKE. A modified version of the Blowfish block cipher is recommended as one of the ciphers supported.

3.3 NDS

The NDS proposal covers all three layers of the DPS requested by the DTDG CFP. This proposal has a broader scope than just digital transmission content protection as it supports an encrypt-once feature which does not require an encryption function in the CE/IT devices. However, local link encryption/decryption is also supported.

3.3.1 CCI

A CopyRight String (CRS), containing CCI and, if desired, other copyright information, is used in content decryption to ensure its integrity.

3.3.2 Authentication and Key Exchange

The AKE is based on public key techniques: zero-knowledge Fiat-Shamir Authentication; RSA is suggested for exchanging session keys between the authorized devices. The authentication can automatically verify CCI data and public keys. The blacklisting of rogue devices and clones, as well as key recovery are supported.

3.3.3 Content Encryption

This proposal suggests using either the DVB Common Scrambling Algorithm and/or the well known DES ciphers. Alternate ciphers can be supported as well. Infrastructure for upgrades is provided. With this proposal's encrypt-once feature the content is encrypted once-only by the source, and needs to be decrypted only at the final play-out device. Between the source and the final destination only the decryption key is re-encrypted at each link with the local session keys.

3.4 PictureTel

The PictureTel proposal covers all three layers of the DPS requested by the DTDG CFP.

3.4.1 CCI

CCI can be exchanged between devices via both embedded and control channel mechanisms. Message authentication using a keyed SHA-1 hash is used to ensure the integrity of CCI carried by the control channel. Embedded CCI can be exchanged between devices in the clear as its integrity is protected by making correct decryption by the content be dependent on it being received unaltered.

3.4.2 Authentication and Key Exchange

The AKE layer provides mutual authentication and key exchange, and is based on Public Key cryptographic techniques including RSA Digital Signatures and a variant of Diffie-Hellman Key Exchange called the Lightweight Public Key Agreement Protocol (LiPKAP). Certificate revocation capability is provided. In addition, an optional key recovery mechanism is supported to enable the recovery of device keys on demand by the authorities.

3.4.3 Content Encryption

A family of stream ciphers are proposed which offer a range of performance and implementation cost tradeoffs. NFSM-128 is a derivative of the WAKE-ROFB cipher and NFSM-160W is a derivative of the WiderWake cipher.

4. Technical Evaluation of Proposals

This section contains, in table form, information provided by the proposers in response to the Request for Supplemental Evaluation Data, which was issued by the DTDG on July 24, 1997. The entire Request for Supplemental Evaluation Data is contained Appendix C of this recommendation.

The information as presented in the tables in this section was reviewed and edited by each of the proposers during the DTDG meeting in September 18 and 19, 1997.

4.1 Content Encryption/Decryption

This section contains information about the encryption layer of each proposal. The information in this section includes implementation complexities in hardware and in software, as well as some robustness and error handling information.

4.1.1 Hardware Implementation

"OUTSIDE COUNSEL'S EYES ONLY"

S 00037

	Regs # and size	# size and function of arith. func	# bits RAM, ROM, FIFO and/or NVRAM	Misc logic (gate count)	Total gate count (optional)	Performance
Hitachi/ Matsushita/ Sony	M6-CCBC:381 bits total (3048gates)	M6-CCBC:2 32 bit ADDERs, 72 2 input XORs (664gates)	M6-CCBC:0	M6-CCBC:208 2 input selectors, 64 3 input selectors, 64 4 input selectors, etc. (1934Gates)	M6-CCBC: 5646gates	M6-CCBC: 32Mbps @ 25MHz
Intel / Toshiba	224 bits total	1 32 bit adder, 128 2 input XORs	1 KB RAM, 40 Bytes of FIFO	168 bits of 2 to 1 mux 250 gates for control logic and state machine	3 Kgates + 1 KB RAM + 40 Byte FIFO	32Mbps @ 25MHz assuming no key updates
NDS DVB Decryption only DES figures can be acquired from the literature	2X8B control word per service	N/A	None	10-12Kg	10-12Kg (not including regs)	80Mbps
PictureTel	NFSM-128: 128 bits total	32 bit adder, 56 2 input XORs	512 bits RAM, no ROM, no FIFO (est. equivalent to 512 to 768 gates depending on method of counting)	40 2 input muxes, 5 bit state machine (220 gates [LCB500K])	Based on LSI Logic LCB500K cell libraries: 1016 gates + 512 RAM bits≅ 1528 gates	200Mbps @ 25 MHz

When reviewing the total gate count entry in the table above, it is important to note two important points:

1) Although the official Request for Supplemental Evaluation Data attempted to define a gate as a 2 input NAND gate made with 4 transistors, more than one of the proposers expressed uncertainty about how to use this metric to calculate a gate count for implementing their method.

2) The DTDG did not ask the proposers to describe how they calculated gate count or any of the other information in this section. It is possible, therefore, that some of the information in this table is derived from functioning prototypes while other information is based on estimates based on a paper design. The DTDG makes no comment as to the accuracy or usefulness of the information in this table or in any other are of this recommendation.

Taking into account this situation, the figures found in the column for total gate count should be studied with some uncertainty. Note that the DTDG has chosen to treat this information as optional.

4.1.2 Software Implementation

	Time to encrypt 200B, 64KB, 8MB (memory to memory in place)	Time to decrypt 200B, 64KB, 8MB (memory to memory in place)	Initialization time	RAM requirements for execution (executable code, temp RAM, fixed tables, keys)	Processor
Hitachi Matsushita/ Sony	200B:7.4us 64KB:2.5ms 8MB:360ms 200B:207Mbps 64KB:208Mbps 8MB:176.5Mbps	200B:7.9us 64KB:2.6ms 8MB:380ms 200B:194Mbps 64KB:194Mbps 8MB:165Mbps	2.6us	code:1.5KB RAM:88B tables:none keys:8B	266Mhz Pentium II processor L1:32KB L2:512KB
Intel/ Toshiba	200B:11.0us 64KB:3.5ms 8MB:501ms 200B:146Mbps 64KB:150Mbps 8MB:134Mbps	same	15us	code:3.8KB RAM:incl. tables:incl. keys:incl total:3.8KB	266Mhz Pentium II processor L1:16BKi, 16KBd L2:512KB
NDS DVB Decryption only DFS figures can be acquired from the literature	not relevant for DVB	200B:not done 64KB:3S 8MB:370S *200B:* *64KB:170.67Kbps* *8MB:172.97Kbps*	included in estimate for DVB	code: RAM: tables: keys: total:9KB	100Mhz Pentium class processor L1:? L2:256KB
PictureTel	200B:2.79us 64KB:864us 8MB:183ms 200B:573Mbps 64KB:606Mbps 8MB:366Mbps	same	<10us	code:1KB RAM:incl tables:<1.5KB keys:incl. total:<2.5KB	266Mhz Pentium II processor L1:16KBi, 16KBd L2:512KB

Note that the values in the table above which are written *in italics* are calculated from the information provided by the proposer, which appears in normal text in the same cell. Any discrepancy between the value in italics and the information in the same cell which is in normal text is unintentional; in this case, the information in normal text should be used.

4.1.3 Robustness Characteristics

	Variable keys?	Cipher text attack, known plain text, chosen plain text
Hitachi/ Matsushita/ Sony	40 to 64bits	Case 1: known plain text attack - key exhaustive search, data key 2^^39; key encrypting/service keys 2^^63 or more Case 2: chosen plain text - differential/ linear attacks; more than case 1
Intel/ Toshiba	40 to 128bits	No known structural weaknesses of blowfish, some known weak keys which can be avoided
NDS	up to 64b (same as DVB)	Better than DES, according to DVB robustness evaluation results
PictureTel	40 to 128bits	Known ciphertext attack: Greater than 2^^40 operations for exhaustive search on shortest recommended key. Up to 2^^128 operations for longest key, subject to export approval. Known plaintext attack: estimated to require more than 2^^39 bytes of known plaintext (>500GBytes) under same key. Chosen plaintext attack: stream cipher mode makes this the same as known plaintext attack, except that if _adaptive_ chosen plaintext is deemed an applicable attack mode then cipher stream re-synchronization should be from dedicated IVs rather than solely from the ciphertext as tentatively proposed. Iterative cipher structure allows additional resistance to known/chosen plaintext attack for a proportionate reduction in speed, without needing additional hardware.

Note that the table in this section does not contain all the information requested in the Request for Supplemental Evaluation Data. Specifically, the columns titled "Protect Embedded CCI" and "Minimum Key Entropy" are now removed from this table. The rational for this removal is described in the following text.

In the case of "Protect Embedded CCI", the co-chairs observed that the embedded CCI is actually part of the AV data stream. As such, the encryption layer automatically protects this embedded CCI by the same means that the AV data itself is protected. In addition, the

proposers did not consistently respond to this question. The co-chairs of the DTDG felt, therefore, that the information which was remaining in this column was not useful, and was to some extent misleading.

In the case of the "Minimum Key Entropy" column, almost none of the proposers responded with information for this category because the requested information was not clearly defined. Because of this, the co-chairs decided to remove this column from the final recommendation.

4.1.4 Error Handling Characteristics

	effect of bit errors?	Error propagation within a packet	Error propagation from one packet to the next
Hitachi/ Matsushita/ Sony	Corresponding source packet is lost	two blocks (128bits total) or less	none
Intel/ Toshiba	IEEE 1394 packet is dropped	to end of 64 bit cipher block	none
NDS	limited to a single MPEG2 transport packet	To end of transport packet	only if transport packet extends to next bus packet
PictureTel	cipher has no error propagation, but IEEE 1394 may drop CRC error packets	same as bit error effect	only if error is in resynch data

4.2 Device Authentication and Key Exchange

4.2.1 Hardware Implementation

Given that none of the proposers recommend that their proposed authentication layer be implemented in hardware, the DTDG co-chairs concluded that the space information that is available in this area should not be included in a recommendation.

4.2.2 CE Software Implementation

	Time for Authentication and Key Exchange (processor used)	RAM required	ROM required
Hitachi/ Matsushita/ Sony	Common key:105ms (H8/3337T @ 3Mhz) Public Key (indirect):1.269s (27Mhz, 32bit CPU)	Common key: 200B Public key: to be measured	Common key: 1.8KB Public key: 12.9KB
Intel/ Toshiba	14ms Preliminary AKE (12 MHz 80286) 17s Full AKE (8 MHz 80286)	1.2KB	8.8KB
NDS	510ms for 512bit modulus, 2s for 1024 bit modulus for checker per round times 20 rounds (4 MHz 80188) 560ms for 512b modulus, 2.2s for 1024b modulus for prover per round, times 20 rounds (4 MHz 8051) Does not include RSA key exchange	70 to 100B for checker 70 to 140B for prover Does not include RSA for key exchange	273B min, additional 425 for additional features for checker 512B for prover Does not include RSA for key exchange
PictureTel	44ms (25Mhz 80486)	~1KB	<4KB ROM for code (est.), ~1 KB EPROM (or EEPROM) for public key certificates, 16 to 32 bytes of secure EPROM/EEPROM for device key (Private key)

4.2.3 IT Software Implementation

	Time for Authentication and Key Exchange (processor used)	RAM required (including code)
Hitachi/ Matsushita/ Sony	Common key: 15us (166Mhz Pentium class processor) Public key: 62.5ms (100Mhz Pentium class processor)	Common key: 1.5KB Public key: 28.5KB code, couldn't measure temporary space
Intel/ Toshiba	22us Preliminary Authentication (266 MHz Pentium II Processor) additional 135ms for Full Authentication (120 Mhz Pentium processor)	< 20KB
NDS	9ms 512b modulus per round, 18ms 1024b modulus per round (100Mhz Pentium class processor, 256KB L2 cache)	500B Does not include PSA for key exchange
PictureTel	6ms (120Mhz Pentium class processor)	~1KB

4.3 System Issues

The table below shows some information provided by the proposers with regard to various system issues.

	Smart card required?	Smart card optional/possible?	Key management infrastructure required
Hitachi/ Matsushita/ Sony	No	Smart card possible. Not recommended	Source device has embedded at manufacturing Sink CE device has license key, send ID embedded at manufacturing Sink PC device receives license key from send ID at software installation time
Intel/ Toshiba	No	Smart card possible. Not recommended	license authority for distributing keys and certificates
NDS	No	Optional in end user devices to allow conditional access by function and upgrading security system	yes
PictureTel	No	Smart card possible. Not recommended	yes, license authority for distribution of keys and certificates

5. Findings

This section contains the findings of the DTDG. The findings for each of these layers are covered in a separate subsection. During the process of the meetings, no one has advocated that a viable DPS requires additional layers or may omit any of the three layers discussed below. All standing proposals at the time of this writing address all 3 layers.

With regard to the robustness of the standing proposals, there is no conclusion. This is due in part to the fact that the DTDG did not have the means to objectively compare the robustness of each of the proposals relative to each other. In the absence of other information, it is reasonable to conclude that all of the standing proposals meet the goal of keeping "honest people honest"[4].

5.1 CCI Layer

Each format of digital AV data which has been mapped to a 1394 isochronous channel, including MPEG2 TS, digital audio and digital camcorder SD, HD and SDL formats, provides a means of including copy control information with the transport data. For the purposes of the DTDG, this form of data is referred to as "Embedded CCI". Because embedded CCI is encrypted and protected as thoroughly as the actual copy protected content, there is no explicit need to address its integrity in its embedded form.

The DTDG has considered the need to carry CCI outside of the data field. For purposes of DTDG discussions, this type of CCI is referred to as "Exposed CCI". The purpose of exposed CCI is to anticipate devices which temporarily store copy protected content as simple binary data, without knowledge of the specific format or type of that data. Such devices have no means of learning the value of the embedded CCI and therefore require a means of recognize copy control information to ensure their correct operation when presented with copy protected data. Exposed CCI, along with the combination of exposed CCI with the encryption layer, have been proposed to address this issue.

5.2 Encryption Layer

Section 3.1. of this recommendation contains information provided by the proposers regarding the hardware and software implementation complexity and other aspects of the encryption layer described in each of the proposals.

When reviewing the hardware implementation complexity, it is important to note the comments found at the end of section 3.1.1. More specifically, the discussions on this subject in the DTDG meetings show that when calculating the number of gates required to implement a given encryption method in hardware, no one can be certain that each proposer was able to use a metric that leads to a number which is directly comparable to numbers calculated by other proposers.

It is also important to note that none of the proposals met the target hardware implementation complexity described in the CFP. (CFP Target is 1Kgate, but the actual range was 1.5Kgate to 12Kgate).

When considering the software implementation complexity for each of the proposals in the encryption layer, there is clearly a wide range of performance characteristics and other overheads. While the CFP software performance target is difficult to quantify, most interested parties feel that the performance of the three most efficient ciphers are capable of decrypting an MPEG TS at DVD rates while requiring no more than 3% of the computation for decompression.

---

[4] The expression "Keep honest people honest" is in common use in the proceedings of the DTDG and its parent organization, the CPTWG.

Finally, with regard to error handling characteristics, given the information provided by the proposers, and considering the nature of distribution of AV data to the consumer, none of the proposals has unacceptable performance in this area.

5.3 Authentication and Key Exchange Layer

No agreement on a set of findings has been reached within the DTDG. Instead, brief statements are provided by the proponents of shared secret and the public key AKE techniques.

5.3.1 Statement from Shared Secret AKE Proponents

Asymmetric_AKE should be supported as baseline AKE in the 1394 environment which many kinds of device connected, i.e. PC, video equipment, audio equipment.

Robustness:

When private key has been divulged in the Global Shared Secret key base AKE, there is a threat of circumvention for all the device. However, Asymmetric_AKE can minimize the threat because it uses a combination of service key, license key and node_unique_ID.

The Public_key_AKE improves security by refusing to communicate with those devices whose private keys are revoked using the Certificate Revocation List (CRL) which is made available by the Administration Center. Without CRL mechanism, there is no significant difference between Public_key_AKE and Asymmetric_AKE in terms of the level of difficulty for reverse engineering, etc.

However, specifically in case of CE devices there is no reasonable method to distribute CRL, and no memory available to store the CRL which can grow more and more over time. Therefore, in light of difficulties in operation of revocation mechanism, the robustness achieved by the Public_key_AKE and the Asymmetric_AKE are almost same.

Furthermore, in light of the criteria of "robust enough to prevent casual copying" and the intention shared by the industries participating CPTWG to seek for anti-circumvention legislation to prevent commercial proliferation of circumventing devices, the both AKE meet with the expectation of CPTWG.

Speed:

Asymmetric_AKE is superior to Public_key_AKE as to performance in time elapsing. Especially for usual processors used in CE devices, the time elapsing may cause inconvenience in users' operating devices.

Cost:

The Asymmetric_AKE is superior to Public_key_AKE as to hardware and software resources required for implementation. The cost for implementation increases in Public_key_AKE more powerful CPU, more program ROM and work RAM are needed.

5.3.2 Statement from Public Key AKE Proponents

The Content Protection System (CPS) for 1394 is a critical link in the chain of technologies used to protect content from being copied as it is distributed to the end user. Accordingly, the 1394 CPS must provide robust protection that will not be a weak link between devices that support other content protection mechanisms including DVD, cable, and direct broadcast satellite. As time and technology progress, significant challenges will be encountered while trying to maintain a policy of "keeping honest people honest". To address this the 1394 CPS solution must be scaleable and long lived to ensure interoperability between present and future devices while maintaining a reasonable balance between cost, overhead, and robustness.

Of the range of technical solutions available, only public key cryptographic technologies meet the above criteria. The principal technical advantage of public key is that it allows the assignment of a unique secret per device manufactured. Thus, there is no shared secret contained in a device which, if compromised through reverse engineering or other methods, would violate the overall integrity of the CPS. The compromise of an individual device's secret only allows clones of that specific device to be made. Should this occur, the integrity of the CPS can be maintained through a public key technique known as certificate revocation lists (CRLs). The ability of a public key based 1394 CPS to address future threats including device cloning with techniques such as CRLs illustrates the scalability of the technology. Our analysis indicates that the resources required to implement and administer a public key 1394 CPS, including CRLs, are reasonable for both CE devices and PCs. Over time, the costs associated with these resources will decline even further, but because the 1394 CPS is public key based, it will have the required robustness and scalability to keep "honest people honest."

5.4 Findings on Issues Related to Implementation in Systems

Fundamentally, all of the DPS proposals can include the use of a smart card, however, most proposers do not recommend a smart card as part of the DPS.

Additionally, all DPS systems require some means of managing the distribution of keys to device manufacturers.

The DTDG has been operating under the assumption that there are and will continue to be a variety of means by which content providers will protect their data at the point where it is originally released via pre-recorded media such as DVD, or broadcast such as digital terrestial or digital satellite.

All the proposals address the requirements established in the CFP for a three layer device to device DPS. In addition, the NDS proposal defines an end to end (original content source to final display device) DPS, sometimes referred to as "Encrypt Once". Except for the "Encrypt Once" element of the NDS proposal, none of the proposals are affected by the details of how content providers protect their data at the point where it is originally released. In contrast, the "Encrypt Once" DPS requires agreement and cooperation from content providers regarding how copyrighted data is protected at its point of original release. The "Encrypt Once" portion of the NDS proposal relies on a set of assumptions which is significantly different than the assumptions under which the DTDG has been operating.

6. Appendix A: Definition of Terms

Cryptography: science and study of secret writing.

Cipher: secret method of writing that transforms plaintext into ciphertext.

Encryption (encipherment, scrambling): process of transforming plaintext into ciphertext.

Decryption (deciphering, descrambling): process of transforming ciphertext into plaintext.

Cryptanalysis: science and study of breaking ciphers.

Cryptology: cryptography + cryptanalysis.

Cryptographic system (cryptosystem):

A plaintext message space.

A ciphertext message space.

A key space.

A family of enciphering transformations.

A family of deciphering transformations.

Symmetric key cipher: enciphering and deciphering keys are the same or can be easily determined from each other.

Stream cipher: Stream ciphers apply a sequence of keys to transform individual data characters (e.g. typically bits or bytes.) Examples: RC4 and SEAL. Stream ciphers can either be symmetric-key or public key.

Block cipher: Block ciphers apply a fixed (key dependent) transformation to blocks of data. Examples: DES, FEAL, IDEA, and RC5. Block ciphers can either be symmetric-key or public key.

Asymmetric (public) key cipher: enciphering and deciphering keys differ in such a way that at least one key is computationally infeasible to determine from the other. Examples: RSA, ElGamal, and Merkle-Hellman.

Data integrity: property whereby data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source.

Authentication: (1) Message authentication, (2) Entity authentication.

Message authentication (data origin authentication): type of authentication whereby a party is corroborated as the original source of specified data created at some time in the past (by definition, message authentication includes data integrity).

Entity authentication (identification): type of authentication whereby one party is assured of the identity of a second party involved in a protocol, and that the second has actually participated.

Digital signature: data string which associates a message with some originating entity.

Digital signature scheme: signature generation algorithm + associated verification algorithm.

Two general classes of digital signature schemes: (1) digital signature schemes with appendix, (2) digital signature schemes with message recovery.

Digital signature scheme with appendix: DS scheme which requires the message as input to the verification algorithm. Examples: DSA, ElGamal, and Schnorr.

Digital signature scheme with message recovery: DS scheme which does not require a priori knowledge of the message for the verification algorithm. Examples: RSA, Rabin, Nyberg-Rueppel.

REFERENCES

(1) **Cryptography and Data Security**, D. E. R. Denning, Addison-Wesley, 1983.

(2) **Security in Computing**, C. P. Pfleeger, Prentice-Hall, 1989.

(3) **Security for Computer Networks**, D. W. Davies and W. L. Price, John Wiley and Sons, 1989.

(4) **Secure Data Networking**, M. Purser, Artech House, 1993.

(5) **Practical Computer Network Security**, M. Hendry, Artech House, 1995.

(6) **Network Security**, C. Kaufman, R. Perlman, and M. Speciner, Prentice Hall, 1995.

(7) **Applied Cryptography**, B. Schneier, John Wiley and Sons, 1996.

(8) **Handbook of Applied Cryptography**, A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, CRC Press, 1997.